IN THE CLAIMS:

1. (previously presented) A system including at least two parts or stations wherein a transaction or connection between any two or more of said parts or stations is automatically conducted or established by means of an access code, said access code being available to an accessed part or station and requiring an identical access code to be provided to an accessing part of station at the time of conducting the transaction or establishing the connection, wherein said access code is one of a plurality of codes provided to said accessed part or station and available to said accessing part or station, wherein said access codes can be infinitely refreshed, said access code being selected from said plurality of codes at the time of conducting the transaction or establishing the connection such that no two transactions are conducted or no two connections are established with the same access code, and wherein if an identical access code is not provided, the accessed part or stations requests three more access codes from the plurality of codes at the accessing part and requires an identical match with a subsequent three access codes at the accessed part in order to conduct the transaction or establish the connection, such that said previously used codes are not deleted but remain in an active state of service.

2. (previously presented) A system according to claim 1 wherein said selected code is disabled after it has been used to conduct a transaction or establish a connection between said accessed and accessing parts or stations.

3. (previously presented) A system according to claim 1 wherein said plurality

of codes is generated by means of a pseudo random generator.

4. (previously presented) A system according to claim 1 wherein said plurality of codes is generated by means of a software program arranged to produce non-repeating sequence of codes.

5. (previously presented) A system according to claim 1 wherein each code includes a sequence of characters and numbers.

Claim 6 (cancelled).

7. (previously presented) A system according to claim 1 wherein the plurality of codes is generated external to said system.

8. (previously presented) A system according to claim 1 wherein said plurality of codes is at least 100.

9. (previously presented) A system according to claim 1 including first code storage means associated with said accessing part or station for storing one copy of said plurality of codes.

10. (previously presented) A system according to claim 9 including second code

storage means associated with said accessed part or station for storing a second copy of said plurality of codes identical to said one copy stored in said first storage means.

11. (previously presented) A system according to claim 9 wherein said first code storage means includes one of an ATM transaction card, a smart card, an integrated circuit microchip and a computer diskette.

12. (previously presented) A system according to claim 10 wherein said second code storage means is associated with one of a bank computer system, a service provider computer system and a telephone exchange.

13. (previously presented) A system according to claim 1 wherein at least one said part or station includes an ATM terminal.

14. (previously presented) A system according to claim 1 wherein at least one said part or station includes a PC or computer terminal.

15. (previously presented) A system according to claim 1 wherein at least one said part or station includes a mobile transceiver.

16. (previously presented) A system according to claim 1 wherein at least one said part or station is associated with a door opening apparatus.

17. (previously presented) A method of automatically conducting a transaction or establishing a connection between at least two parts or stations by means of an access code, said access code being available to an accessed part or station at the time of conducting the transaction or establishing the connection and requiring an identical access code to be provided to an accessing part or station, said method including the steps of:

making available a plurality of codes to said accessed and said accessing parts or stations;

selecting, at the time of conducting the transaction or establishing the connection, one code from said plurality of codes;

using said selected code to conduct the transaction or establish the connection such that no two transactions are conducted or no two connections are established with the same access code; wherein

said previously used codes are not deleted from said accessing and accessed parts and stations but remain in an active state of service;

said access codes being present in storage means and memory devices selected from the group consisting of integrated circuit microchips, smart cards, magnetic strips, ATM cards and diskettes associated with the accessing part, wherein the accessing part is selected from the group consising of mobile transceivers, Automated Teller Machine terminals, personal computers and door opening apparatus;

infinitely rejuvenating and refreshing with new codes via auto-loading; and

verifying said access codes by an interactive multiple strike challenge-response mechanism.

18. (previously presented) A method according to claim 17 wherein said selected code is removed from said accessed part or station or is otherwise disabled after it has been used to conduct a transaction or establish a connection between said accessed and accessing parts or stations.

19. (previously presented) A method according to claim 17 wherein said plurality of codes is generated by means of a pseudo random generator.

20. (previously presented) A method according to claim 17 wherein said plurality of codes is generated by means of a software program arranged to produce non-repeating sequence of codes.

E1

21. (previously presented) A system according to claim 17 wherein each code includes a sequence of characters and numbers.

Claim 22 (cancelled).

23. (previously presented) A method according to claim 17 wherein the plurality of codes is generated external to said at least two parts or stations.

24. (previously presented) A method according to claim 17 wherein said plurality of codes is at least 100.

25. (previously presented) A method according to claim 17 including providing first code storage means associated with said accessing part or station for storing one copy of said plurality of codes.

26. (previously presented) A method according to claim 25 including providing second code storage means associated with said accessed part or station for storing a second copy of said plurality of codes identical to said one copy stored in said first storage means.

E1

27. (previously presented) A method according to claim 25 wherein said first code storage means includes one of an ATM transaction card, a smart card, an integrated circuit microchip and a computer diskette.

28. (previously presented) A method according to claim 26 wherein said second code storage means is associated with one of a bank computer system, a service provider computer system and a telephone exchange.

29. (previously presented) A method according to claim 17 wherein at least one said part or station includes an ATM terminal.

30. (previously presented) A method according to claim 17 wherein at least one said part or station includes a PC or computer terminal.

31. (previously presented) A method according to claim 17 wherein at least one said part or station includes a mobile transceiver.

32. (previously presented) A method according to claim 17 wherein at least one said part or station is associated with a door opening apparatus.

Claims 33-34 (canceled)

35. (previously presented) A method of establishing a secure connection between a provider and a customer, comprising the steps of:

providing a magnetic strip on a card for storing a first set of codes with the customer;

providing a computer for storing a second set of codes with the provider, said second set of codes being identical to the first set of codes;

receiving a first code from the customer during establishing the secure connection, the first code being selected from the first set of codes without manual customer intervention;

accessing a second code from the second set of codes;

comparing the first code with the second code, wherein a perfect match is a successful verfication; and

preventing further use of the first code by the customer by disabling the first code and the second code without manual customer intervention.

Claim 36 (cancelled).

Please add the following new claims:

37. (previously presented) A method as recited in claim 35, further comprising the steps of:

activating a code replacement module within the computer based upon a triggering event, wherein the triggering event is disabling of a specified number of codes; and

automatically loading new codes onto the magnetic strip by the code replacement module.

38. (previously presented) A method as recited in claim 35, wherein the automatic loading is an Internet download.

39. (previously presented) A method as recited in claim 35,wherein the automatic loading is conducted between wireless devices.

40. (previously presented) A method as recited in claim 35, further comprising the steps of:

performing verifications until all the codes are used up or spent;

providing a second magnetic strip to the customer, the second magnetic strip having a third set of codes;

replacing the magnetic strip on the card with the second magnetic strip; and

storing in the computer a fourth set of codes identical to the third set of codes to allow continuing comparing codes for the perfect match to allow the successful verification, wherein the third and fourth set of codes never can have a code that has been used before.

41. (previously presented) A code based door opening apparatus for a safe room comprising:

a portion that is inaccessible to a user for controlling access to the safe room;

first means within the portion for storing a first set of codes;

second means in possession of the user for storing a second set of codes, wherein when the user requires access the safe room, the second means serves as an electronic key to gain access by providing an unused code to the portion, said portion requiring an identical unused code from the first means to grant access to the safe room, wherein the first set of codes may be automatically refreshed based upon a triggering event such that each code is used only once.

42. (previously presented) A system according to claim 17 wherein said selected code is deactivated and decommissioned after said selected code has been used to conduct a transaction or establish a connection between said accessed and accessing parts or stations.

43. (previously presented) A system according to claim 17 further comprising the step of initially receiving a password to serve as a primary level of security between

the accessed part and the accessing part.

44. (previously presented) A system as recited in claim 1, wherein a verification of access codes is conducted separately and independently of a password and PIN verification.

45. (previously presented) A system as recited in claim 1, further comprising software means for generating the access codes within a spreadsheet program, wherein, a pattern of character and numbers are manually mixed in a manipulated combination process to generate access codes.

46. (previously presented) A system as recited in claim 45, wherein the software means is externally located to the accessing and accessed parts.

47. (previously presented) A system as recited in claim 45, wherein upon completion of download or transfer of additional aaccess codes from said software means

a self-destruct mechanism is automatically activated by the softwaremeans to permanently remove and delete all traces of said access codes.

48. (previously presented) A method as recited in claim 45, wherein the access codes are refreshed in groups of 500.

49. (previously presented) A fully automatic method of establishing a secure connection between a provider and a customer, comprising the steps of:

providing an active memory-storage means present on a card for storing a first group of codes associated with a customer's electronic utility appliance, wherein said active memory-storage means being smart cards and integrated circuit microchips;

said appliances being selected from the group consisting of mobile transceivers, ATM terminals, personal computer and door opening apparatus;

providing a computer for storing a second batch of codes with the provider, said second batch of codes being identical to the first group of codes;

providing a software program verification program running on the computer for selecting, requesting, and receiving a first code from the customer during establishing a secure connection, the requested selected first code being chosen from amongst the first group of codes without manual customer intervention;

accessing a second code from the second group of codes;

comparing the first code with the second code, wherein a perfect match is a successful verification; and

preventing further use of a verified code by the customer by using a verification software program running on the computer to automatically recognize previously used spent codes and to avoid reusing them, wherein previously used codes are not deleted but continues to remain in an active state of service.

50. (previously presented) A method as recited in claim 49, wherein said integrated circuit microchips, may be used as independent, stand-alone memory devices

directly used and associated with said user's electronic utility appliances.

51. (previously presented) A method as recited in claim 49, wherein said memory-storage means may be smart cards.

52. (previously presented) A method as recited in Claim 50, further comprising the steps of:

initiating a trigger mechanism to verify said access codes, said trigger mechanism being a positive verification by PINs and passwords;

using three way transmission traffic during the verification process;

using a real time interactive challenge-response mechanism wherein, verifications are carried out at the point in time of a connection being made, or transaction being conducted;

using an auto-selection mechanism for selecting specific access codes for verification, wherein usage of the codes is managed by a verification software program programmed to disable previously used codes in order to avoid reusing them.

53. (previously presented) A method as recited in claim 52, further comprising of the steps of:

using a fully automated variable access codes verification process without the user's interference or manual work.

54. (previously presented) A system of an automated multiple "strikes"

verification capability comprising:

a verification software module capable of automatically activating and independently launching a series of verifications repeatedly, one after another in quick succession for a triple strike of at least three access codes repeatedly and consecutively until three successively, successful verifications has been obtained in order to establish a secure connection.

55. (previously presented) A system and method as recited in claim 54; wherein said multiple strikes verifications may be initiated by a triggering event;

said triggering mechanism being the failure of an initial verification sequence.

E'

56. (previously presented) A system as recited in claim 55, wherein a memory-storage means retains the codes and the codes are rejuvenated and refreshed with new supplies of access codes; said self-rejuvenative process being automatically initiated and repeated over and over; thus ensuring and guaranteeing a perpetually inexhaustible supply of fresh access codes for verification; wherein the codes are rejuvenated by

maintaining a stockpile of fresh groups of new access codes in support of an automated self-loading mechanism;

a trigger mechanism initiated by a low number of fresh access codes remaining in the storage memory devices; wherein, the

self-rejuvenating mechanism enabled by the auto-loading capability of said software program is automatically activated; wherein, "spent" access codes that have been previously used, are replaced, rewritten and topped up with fresh access codes;

means of an auto-select mechanism wherein, one fresh group of new access codes is automatically selected out of a stockpiled reserve of 1,000 groups, for delivery and conveyance via electronic communications systems and means such as the Internet directly into the end-user's utility appliances such as mobile transceivers, Automated Teller Machine terminals, personal computers, and associated storage means and memory devices such as ATM cards, smart cards, integrate circuit microchips, magnetic strips and computer diskettes.

57. (previously presented) A system as recited in claim 56, wherein, performing verifications until a last access code is left; wherein,

E'

a verification process utilizing the last access code serves to act as the trigger mechanism, prompting the service provider's verification software to initiate an auto-selection and thereafter an auto-loading sequence; after the user has been verified, to select a fresh group of access codes and loading the fresh group directly into the user's electronic utility appliances and storage-memory means.

58. (previously presented) A system as recited in claim 56, wherein an auto-selection mechanism is initiated for choosing at random, one specific group of new access codes out of the reserved 1,000 groups of access codes stockpiled for auto-loading.

59. (new) A system as recited in Claim 56, further comprising of an auto-loading mechanism of the software program which is activated after the user has been verified; wherein

said first part of the plurality of access codes is delivered and auto-loaded into the user's electronic utility appliances and the first storage means; wherein

said delivery means being wireline electronic communication systems (ATM terminal).

60. (previously presented) A system as recited in Claim 59, wherein said delivery means being a wireless electronic communication systems.

61. (previously presented) A system as recited in Claim 60, wherein said electronic communication systems and means of delivery being the Internet.

E'

62. (previously presented) A system as recited in Claim 61, further comprising the means for storing said access codes from said user's electronic utility appliances into related receiving, or storage-memory means such as diskettes, magnetic strips and ATM Cards, directly associated with said Automated Teller Machine terminals, mobile hand-phones and personal computers.

63. (previously presented) A system as recited in Claim 62, wherein said storage-memory means comprises smart-cards.

64. (previously presented) A system as recited in Claim 62, wherein said storage-memory means comprises integrated circuit microchips.

65. (previously presented) A system as recited in Claim 64, further comprising an auto-loading mechanism wherein, a second part of the plurality of codes, is concurrently assigned, and auto-loaded from a code replacement module (17, 47, 59) into said second codes storage means and the codes storage module (15, 46, 58) associated with the accessed part or station under an address which corresponds to a first storage means as unique identity assigned to each respective user.

66. (previously presented) A system as recited in Claim 54, wherein said system is an electronic key being used in securing, restricting and controlling physical access into a high security area.

67. (previously presented) A system as recited in Claim 66, including a verification software program routine for operating a electro-mechanical door opening apparatus associated with the high security area.